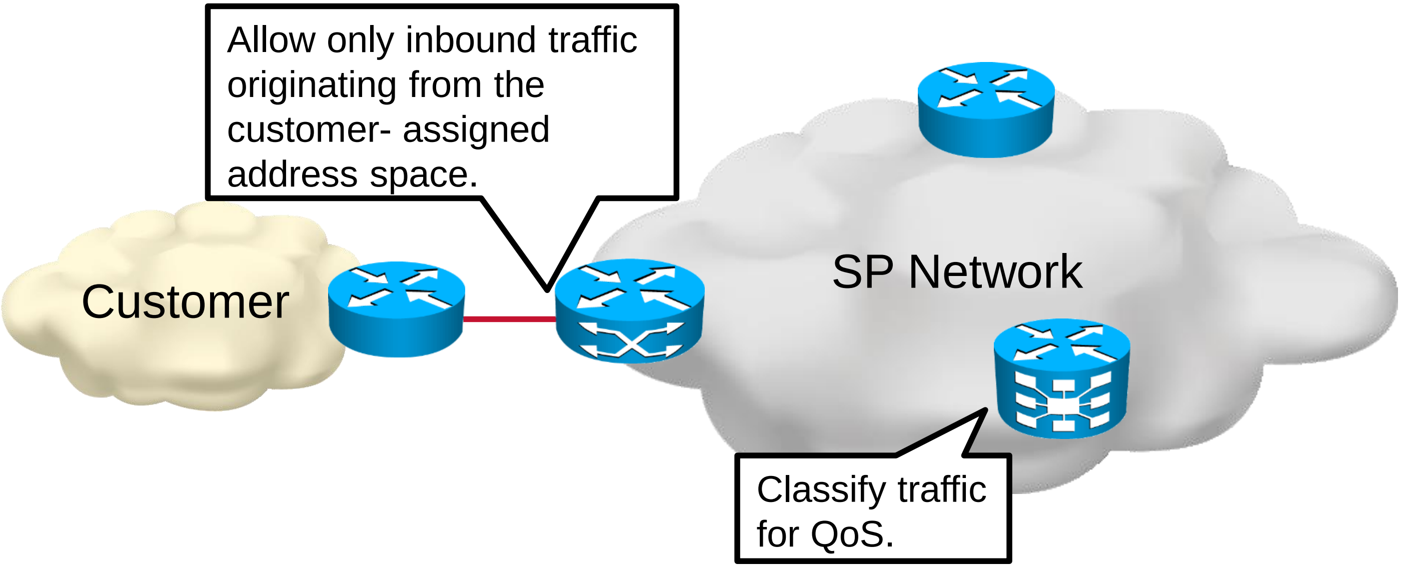
Policy Based Routing

Access Control Lists

ACL Usage

- Filtering:
  - Allows or denies IP traffic by filtering packets through the router interface in one direction
- Classification:
  - Identifies traffic for special handling

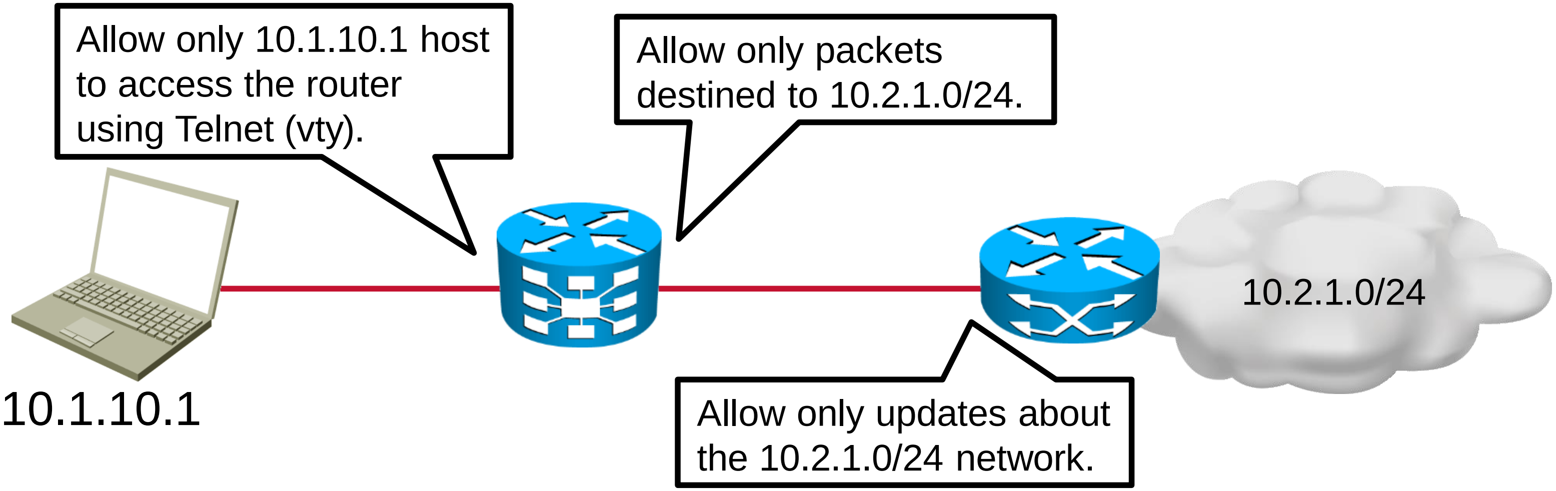


Allow only inbound traffic originating from the customer- assigned address space.

Classify traffic for QoS.

ACL Filtering

- Permit or deny incoming packets on an interface.
- Permit or deny outgoing packets on an interface.
- Control vty access.
- Without ACLs, all packets are allowed to traverse the router interface.



Allow only 10.1.10.1 host to access the router using Telnet (vty).

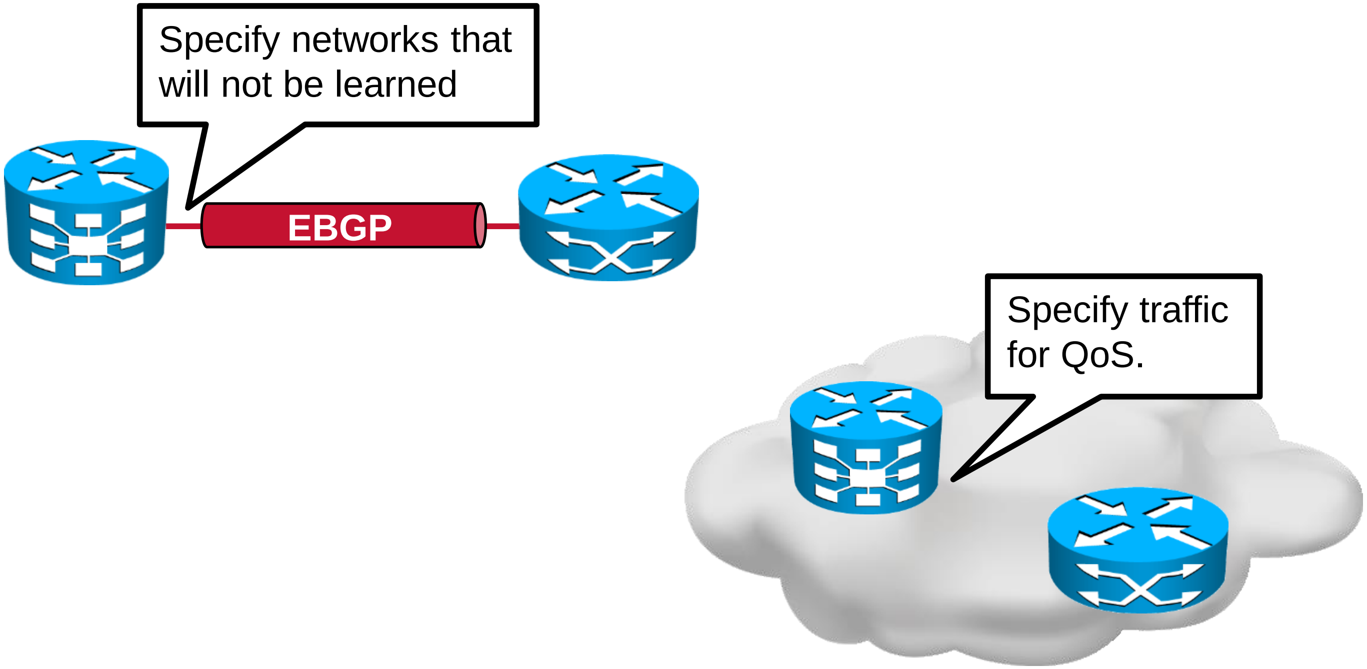
Allow only packets destined to 10.2.1.0/24.

Allow only updates about the 10.2.1.0/24 network.

- Configuration is done in two steps:
  - Create an access list and specify statements.
  - Apply the access list to an interface or line vty.

ACL Classification

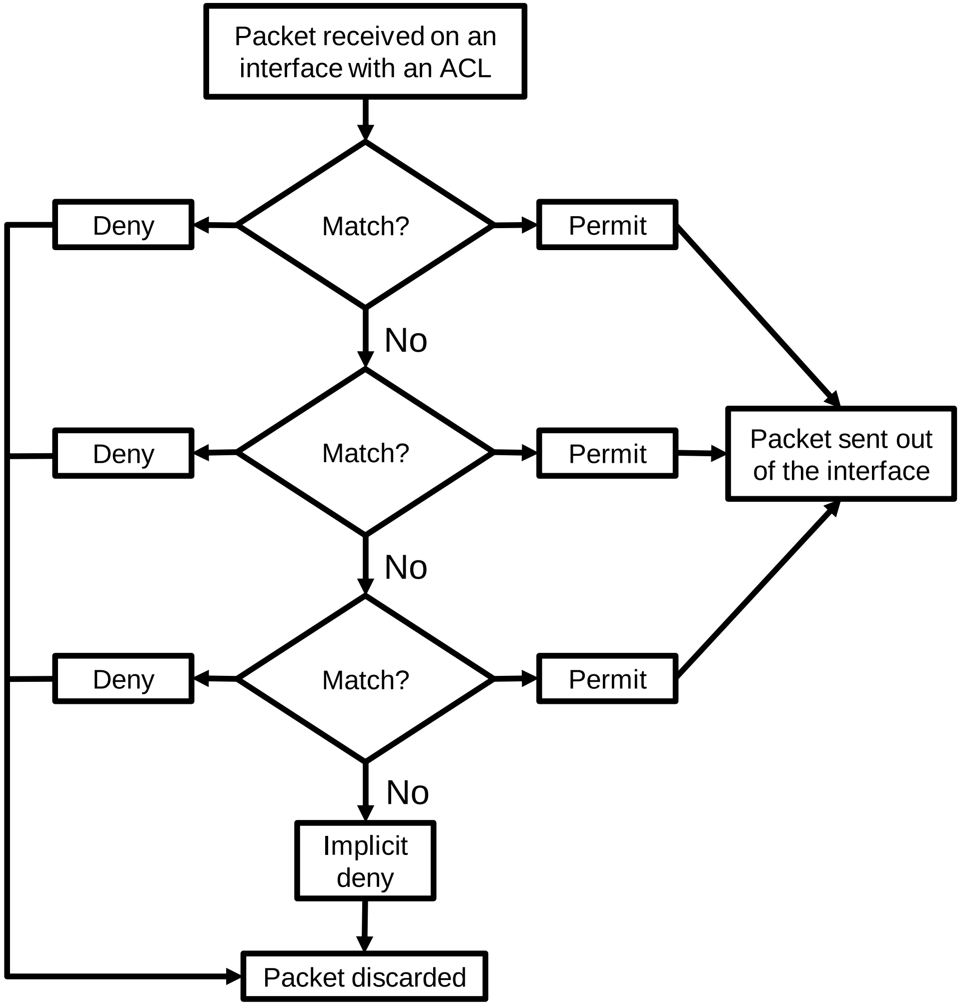
- An ACL classifies traffic that needs special handling.



- Configuration is done in two steps:
  - Create an access list and specify statements.
  - Call/use/reference the ACL in a NAT/Route-map/Policy-map.

ACL Operation

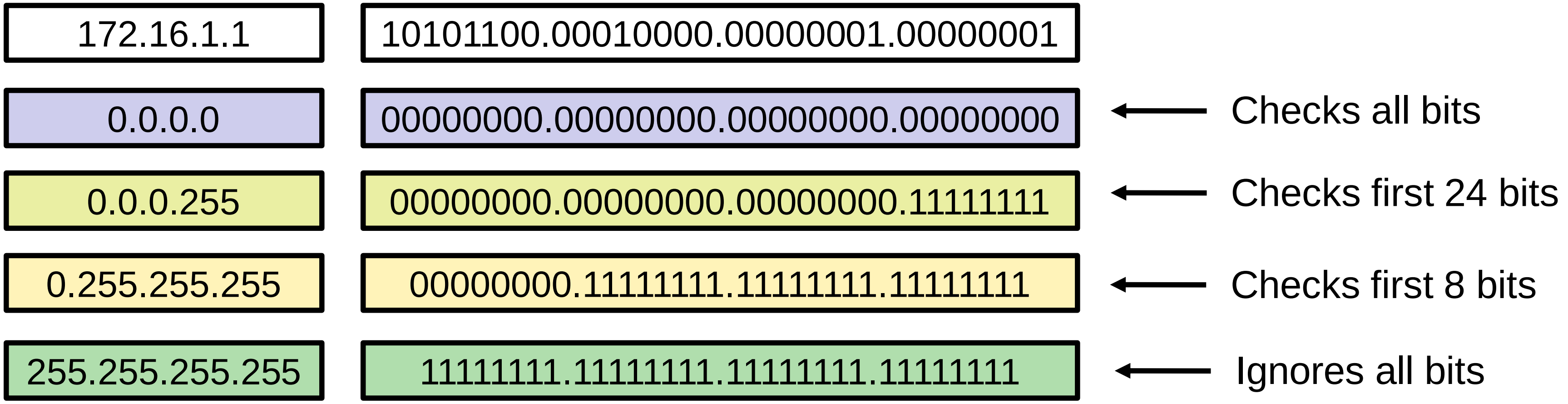
- A ACL is applied to an interface in the inbound or outbound direction.
- An ACL consists of a series of permit and deny statements.
- An ACL is consulted in a top-down fashion.
- First match executes a permit or deny action, and stops further ACL matching.
- **Implicit deny all at the bottom of each ACL.**



```
ip access-list 1 permit 193.136.1.0 0.0.255.255
ip access-list 1 deny 193.136.2.0 0.0.255.255
ip access-list 1 permit host 193.136.3.10
```

Wildcard Mask

- Used together with an IP address in an ACL, it specifies which bits of an IP address in a packet will be checked against an ACL statement:
  - 0 in a wildcard mask means to check a coresponding bit in an IP address.
  - 1 in a wildcard mask means to ignore a coresponding bit in an IP address.
- Two corner cases:
  - Wildcard mask of 0.0.0.0 checks all bits in an IP address (abbreviated as host).
  - Wildcard mask of 255.255.255.255 ignores all bits in an IP address (abbreviated as any).



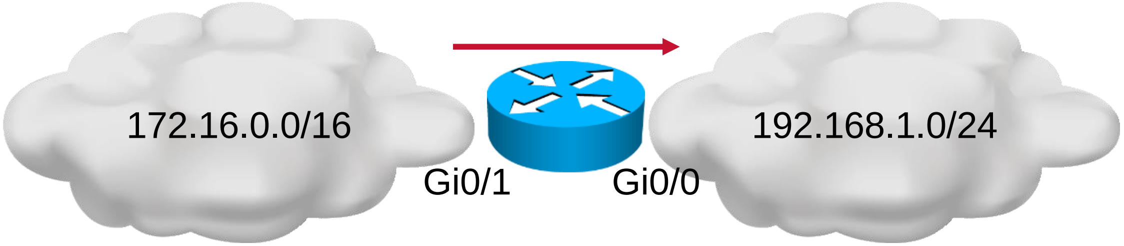
172.16.1.1	10101100.00010000.00000001.00000001	
0.0.0.0	00000000.00000000.00000000.00000000	← Checks all bits
0.0.0.255	00000000.00000000.00000000.11111111	← Checks first 24 bits
0.255.255.255	00000000.11111111.11111111.11111111	← Checks first 8 bits
255.255.255.255	11111111.11111111.11111111.11111111	← Ignores all bits

ACL Types

- Standard ACL
  - Checks only source address
  - Not used often
- Extended ACL
  - Checks source and destination address
  - Checks L4 protocol
  - Checks source and destination port (in case of TCP or UDP)
- ACL identification
  - Numbered ACLs use a number for identification:
    - 1-99 && 1300-1999 Standard ACLs
    - 100-199 && 2000-2699 Extended ACLs
  - Named ACLs use a descriptive number for identification (recommended).

Standard ACLs Configuration Scenario

- Allow only the 172.16.0.0/16 network to communicate with the other network.



```
ip access-list standard FILTER
 10 permit 172.16.0.0 0.0.255.255
 20 deny any
!
interface GigabitEthernet0/1
 ip access-group FILTER in
```

Create a standard ACL.

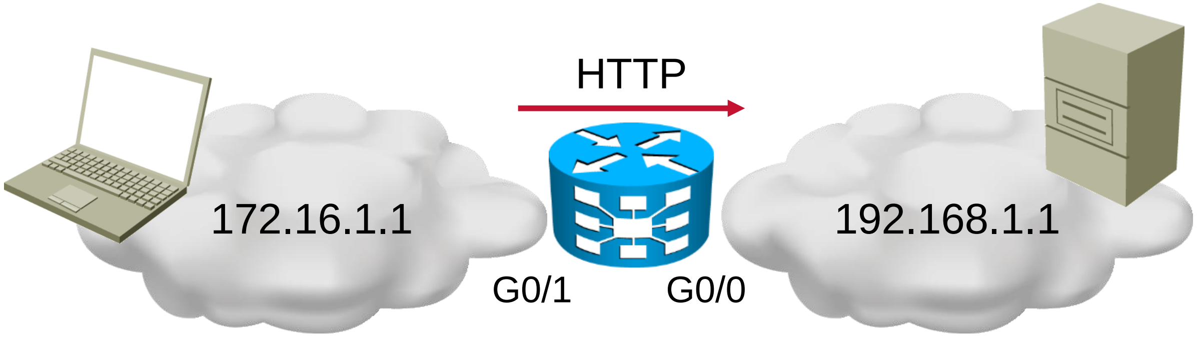
Specify permit or deny statements.

Numbering enables insertion of statements.

Apply the ACL to the interface.

Extended ACLs: Configuration Scenario

- Allow only the 172.16.1.1 host to communicate with the 192.168.1.1 server, using HTTP.
- Only a source port larger than 1023 is allowed to be used by the laptop host.



Create an ACL.

Specify permit or deny statements.

```
ip access-list FILTER
 10 permit tcp host 172.16.1.1 ge 1023 host 192.168.1.1 eq www
 20 deny ipv4 any any
!
interface GigabitEthernet0/1
 ip access-group FILTER ingress
```

source IP operator source port dst. IP operator dst. port

Apply the ACL to the interface.

ACL Guidelines

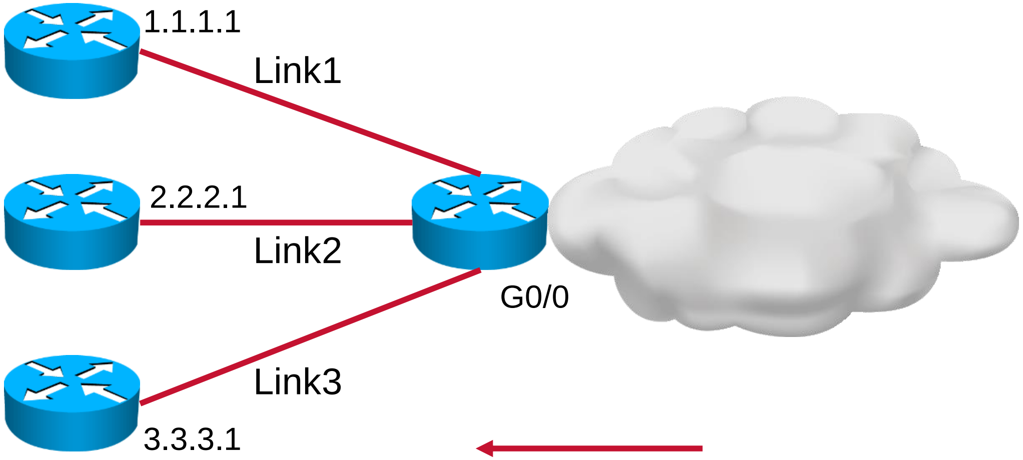
- Standard or extended ACL indicates what can be filtered.
- Only one ACL per interface, per protocol, and per direction is allowed.
- The most specific statement should be at the top of an ACL. The most general statement should be at the bottom of an ACL.
- Due to an implicit deny, an ACL needs at least one permit statement to permit traffic.
- When placing an ACL in a network:
  - Place extended ACLs close to the source.
  - Place standard ACLs close to the destination.
- An ACL applied to an interface does not filter traffic originating from a router; you should apply an ACL to vty lines to limit administrative access (Telnet, SSH) to the router.

Policy Based Routing

Traffic Engineering

Policy Based Routing Example

- The image bellow is a sample topology of a ISP network in which the links have the following bandwidth:
  - Link 1: 10G
  - Link 2: 1G
  - Link 3: 1G



Policy Based Routing Example

- A configuration is required to:
  - Match packets with a source address 5.0.0.0/24 and send them trough link 3.
  - Packets with a source address of 5.0.0.0/24 but with a destination of 6.0.0.0/24 should transverse the link 2.
  - ICMP and SSH (dest. port 22) packets should also be directed to link 2
  - All other traffic should go trough link 1

```
ip access-list extended Net1
 10 permit ip 5.0.0.0 0.0.0.255 any
ip access-list extended Net1-to-Net2-icmp-ssh
 10 permit ip 5.0.0.0 0.0.0.255 6.0.0.0 0.0.255.255
 20 permit tcp any any eq 22
 30 permit icmp any any
```

```
route-map my_RP permit 10
 match ip address Net1-to-Net2-icmp-ssh
  set ip next-hop 2.2.2.1
!
route-map my_RP permit 20
 match Net1
  set ip next-hop 3.3.3.1
```

```
interface g0/1
  ip policy route-map my_RP
```

Policy Based Routing Example (cont)

- In the last example, different but equal ways to finish the route-map:
  - 1) We didn’t specify a last statement, so the route-map has a explicit deny, what happened in the case of PBR is that the forwarding got out of the special PBR lookup and the base normal routing “kicked in”, which means the IGP followed the 10G path.
  - 2) In the bellow example, because we don’t have a match clause, it will match everything and send it trough Link 1.

```
route-map my_RP permit 30
  set ip next-hop 1.1.1.1
```

  - 3) In the last case it will happen the same as 1)

```
route-map my_RP permit 30
```

Policy Based Routing Example Key Knowledge

- Redundant paths, redistribution, and the selected routing protocol all affect network performance. Path control must be enabled to improve performance and avoid suboptimal routing.
- A route map with a group of math and set commands is one of the tools that can be used for path control.
- The path selection process can be accomplished using filters such as route tagging, prefix lists, distribute lists and administrative distance.
- To bypass the routing table destination-based forwarding, PBR is used to determine path selection.
- Path control **match** commands match incoming traffic.
- Path control **set** commands manipulate the path.